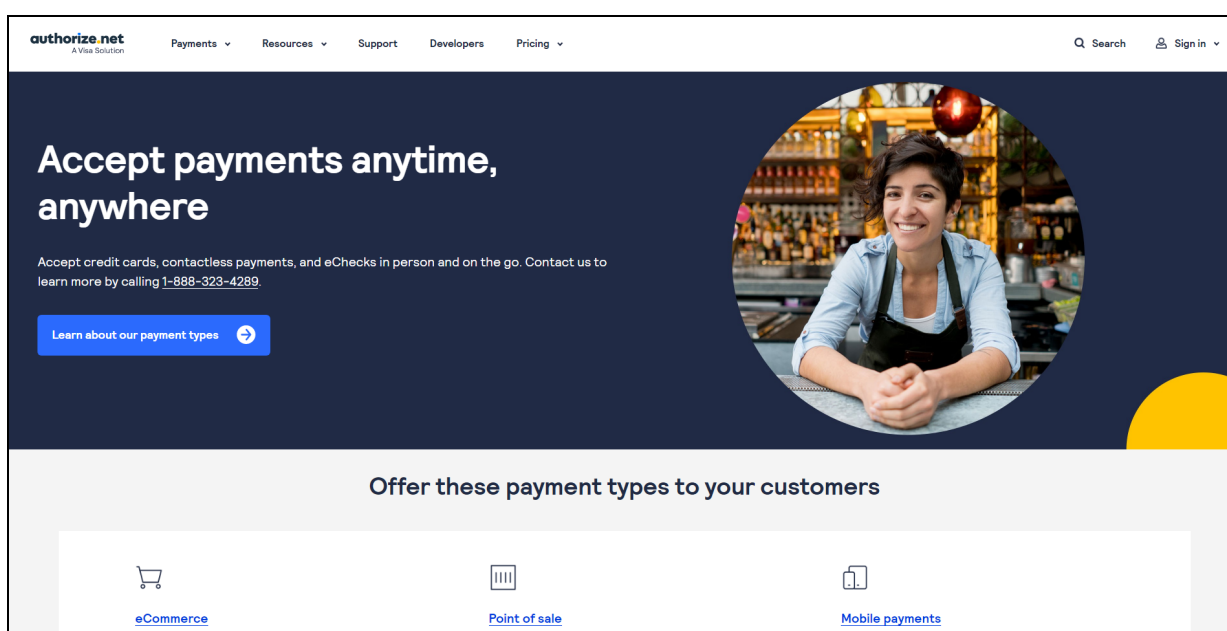


## [Authorize.net API Keys Setup Guide](#)

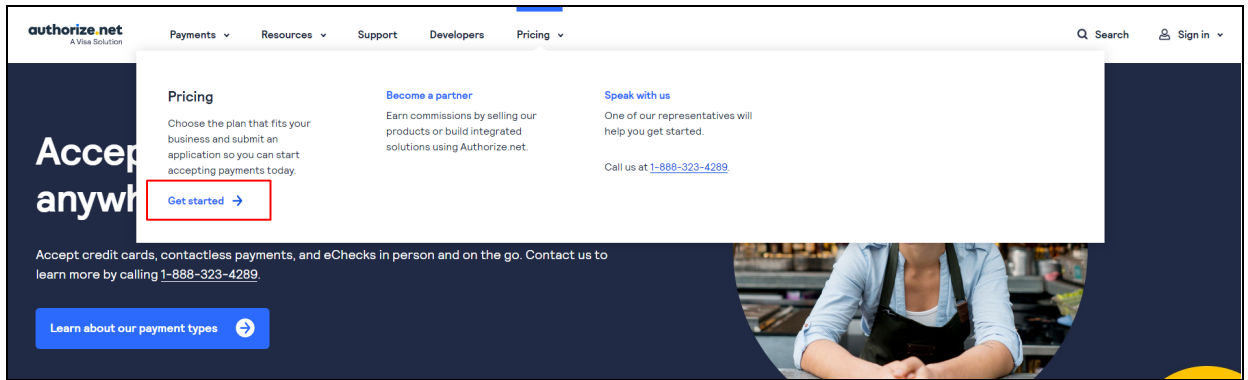
Configure **Authorize.net** keys under **Manage Settings > Payment Methods > Authorize.net > Settings**.

To collect these keys, follow the below steps:

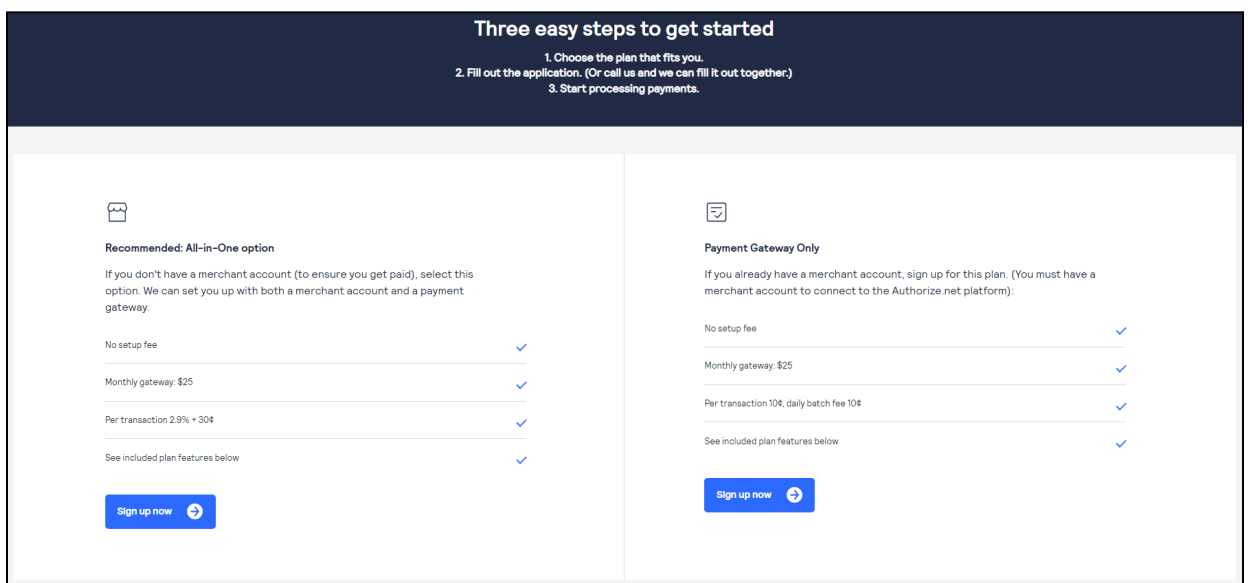
1. Visit <https://www.authorize.net/> and click on **Sign In** from the upper right corner to sign in to your Authorize.net account.



If you don't already have an account, create an account on the website. Hover over the **pricing** option from the header navigation bar and click on **Get Started**.



Select the preferred plan and provide the required details.



**Authorize.Net**

## Merchant Application

Help us understand your business by answering the questions below.

By completing this application, I confirm that I am authorized to submit this application and enter into the agreements linked below on behalf of business indicated.

Tell us about yourself

Owner Name:

Email Address:  Mobile:

Owner Address:

Date of Birth:

Social Security Number:

Primary owner must be a US Citizen with a Social Security Number.

Job Title:

Owner has significant responsibility to control, manage or direct the company

Ownership Percentage:  %  % ⓘ

[+ Add an Owner](#) Complete information on all owners with 25% or greater equity ownership in the company listed below must be disclosed on your application per U.S. Treasury Customer Due Diligence Requirements.

Business name and location

Legal Business Name:

Doing Business As:  Same As Legal Business Name ⓘ

Business Type:

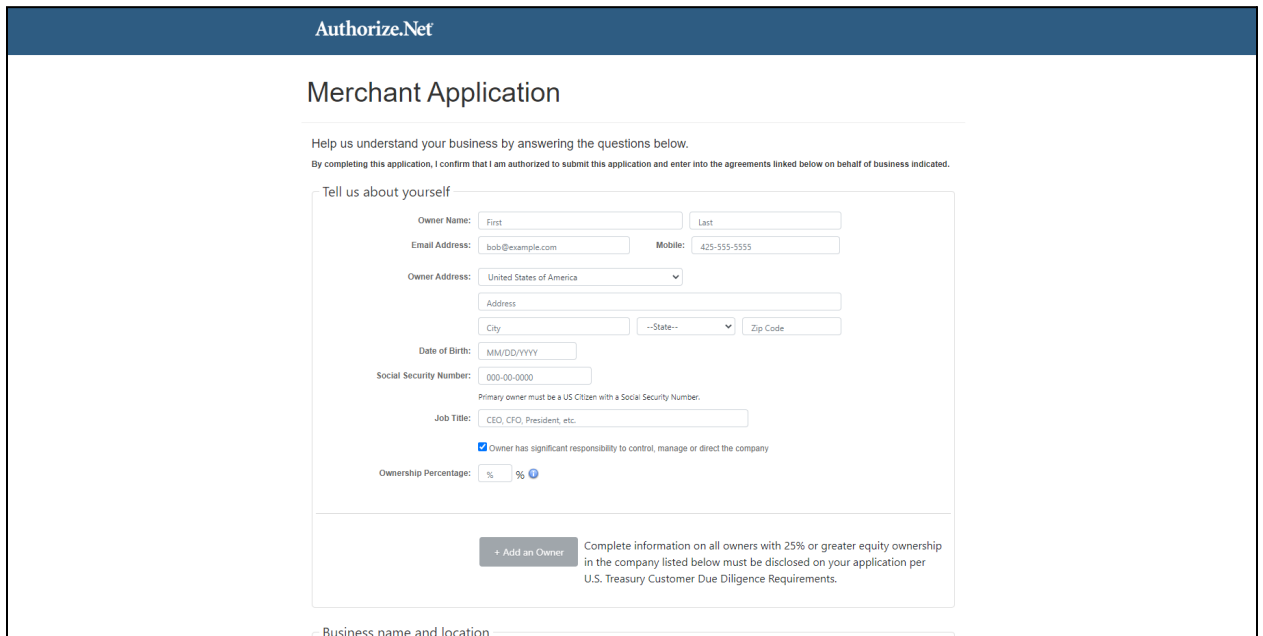
Business Start Date:

Website URL:

Select an account password and log into your account once the account setup is complete.

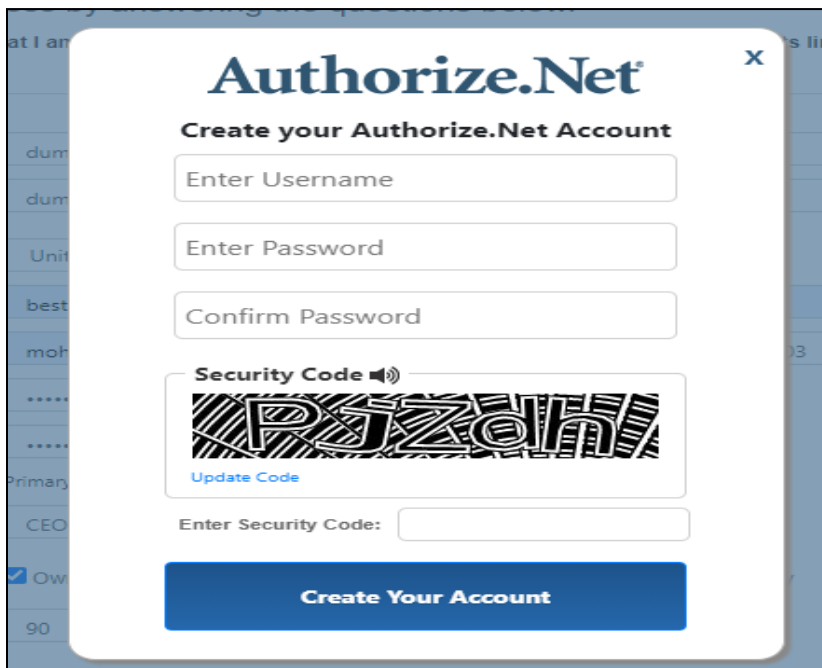
2. Select **'I only have a checking/savings account'** option displayed on the screen.

3. A new page will open. Fill all details and submit it.



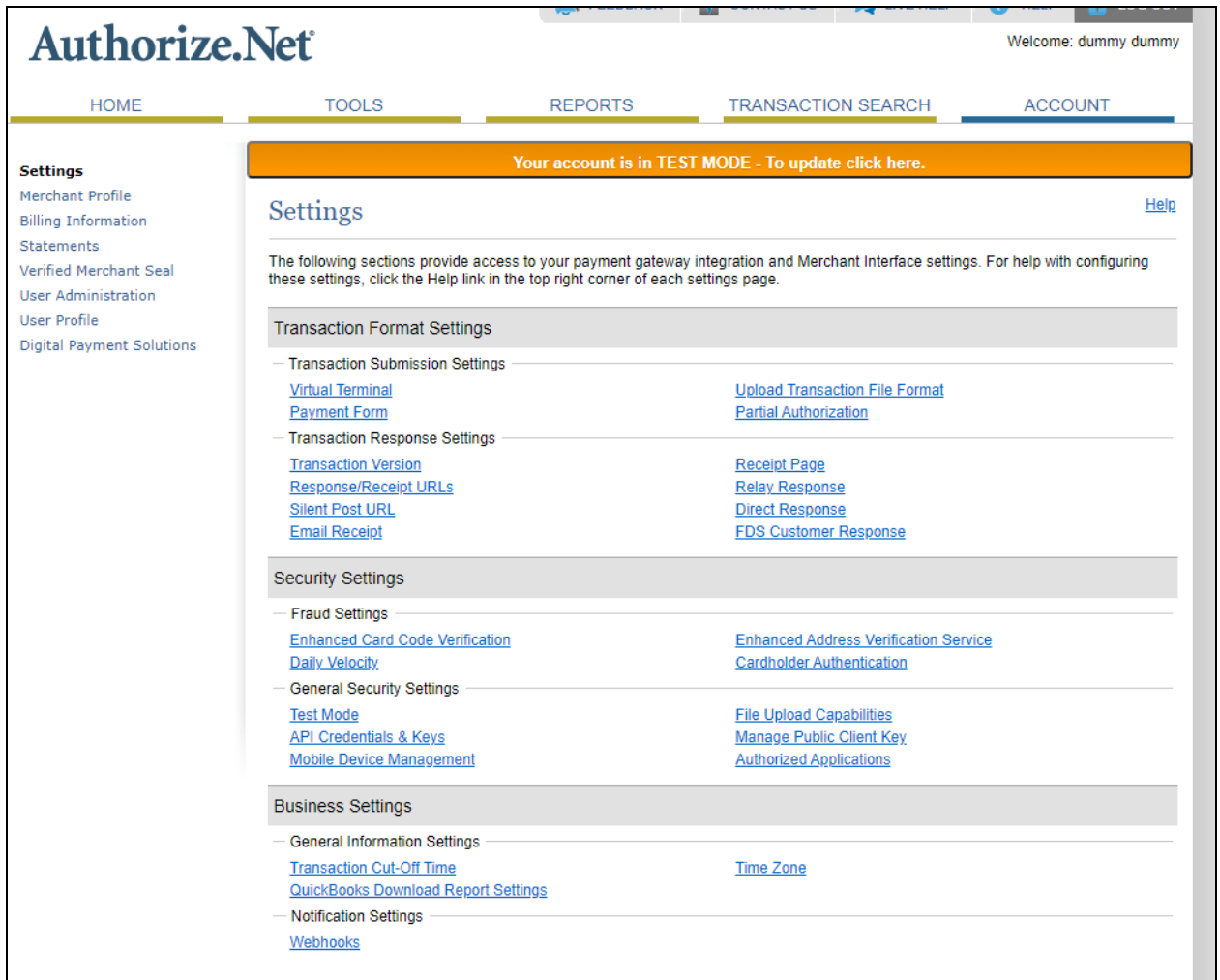
The screenshot shows the 'Merchant Application' page on the Authorize.Net website. The page has a dark blue header with the 'Authorize.Net' logo. Below the header, the title 'Merchant Application' is centered. A sub-header reads 'Help us understand your business by answering the questions below.' Below this is a disclaimer: 'By completing this application, I confirm that I am authorized to submit this application and enter into the agreements linked below on behalf of business indicated.' The main form is titled 'Tell us about yourself' and contains several input fields: 'Owner Name' (split into 'First' and 'Last'), 'Email Address' (with 'bob@example.com' pre-filled) and 'Mobile' (with '425-555-5555' pre-filled), 'Owner Address' (with a dropdown for 'United States of America'), 'Address', 'City', 'State' (dropdown), and 'Zip Code', 'Date of Birth' (MM/DD/YYYY), 'Social Security Number' (000-00-0000), 'Job Title' (CEO, CFO, President, etc.), and 'Ownership Percentage' (with a percentage sign and a help icon). A checkbox is checked, indicating 'Owner has significant responsibility to control, manage or direct the company'. At the bottom of the form is a button labeled '+ Add an Owner' and a note: 'Complete information on all owners with 25% or greater equity ownership in the company listed below must be disclosed on your application per U.S. Treasury Customer Due Diligence Requirements.' The page footer contains the text 'Business name and location'.

4. A pop-up form will open. Fill details and click on 'Create Your Account' button.



The screenshot shows a pop-up form for creating an Authorize.Net account. The form has a white background with a blue border and a close button (X) in the top right corner. The title is 'Authorize.Net' in a large, bold, blue font. Below the title is the subtitle 'Create your Authorize.Net Account'. The form contains four input fields: 'Enter Username', 'Enter Password', 'Confirm Password', and 'Security Code'. The 'Security Code' field is accompanied by a QR code and a speaker icon. Below the QR code is a link that says 'Update Code'. Below the 'Security Code' field is another input field labeled 'Enter Security Code:'. At the bottom of the form is a large blue button with the text 'Create Your Account' in white.

5. Account dashboard page will open.



**Authorize.Net** Welcome: dummy dummy

HOME TOOLS REPORTS TRANSACTION SEARCH ACCOUNT

**Settings**

- Merchant Profile
- Billing Information
- Statements
- Verified Merchant Seal
- User Administration
- User Profile
- Digital Payment Solutions

Your account is in TEST MODE - To update click here.

### Settings [Help](#)

The following sections provide access to your payment gateway integration and Merchant Interface settings. For help with configuring these settings, click the Help link in the top right corner of each settings page.

#### Transaction Format Settings

- Transaction Submission Settings
  - [Virtual Terminal](#)
  - [Payment Form](#)
  - [Upload Transaction File Format](#)
  - [Partial Authorization](#)
- Transaction Response Settings
  - [Transaction Version](#)
  - [Response/Receipt URLs](#)
  - [Silent Post URL](#)
  - [Email Receipt](#)
  - [Receipt Page](#)
  - [Relay Response](#)
  - [Direct Response](#)
  - [FDS Customer Response](#)

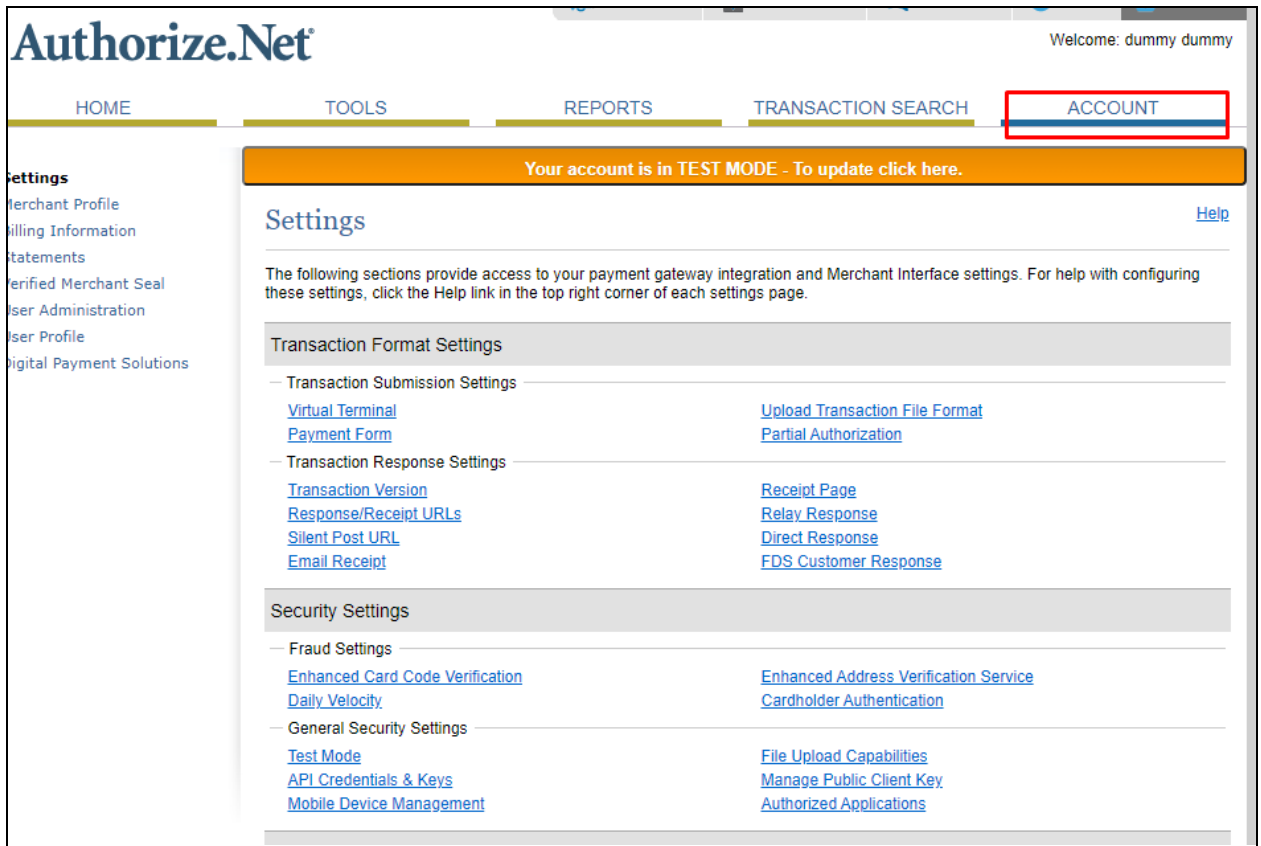
#### Security Settings

- Fraud Settings
  - [Enhanced Card Code Verification](#)
  - [Daily Velocity](#)
  - [Enhanced Address Verification Service](#)
  - [Cardholder Authentication](#)
- General Security Settings
  - [Test Mode](#)
  - [API Credentials & Keys](#)
  - [Mobile Device Management](#)
  - [File Upload Capabilities](#)
  - [Manage Public Client Key](#)
  - [Authorized Applications](#)

#### Business Settings

- General Information Settings
  - [Transaction Cut-Off Time](#)
  - [QuickBooks Download Report Settings](#)
  - [Time Zone](#)
- Notification Settings
  - [Webhooks](#)

6. To obtain Login ID and Transaction Key, click on Account from the main toolbar.



The screenshot shows the Authorize.Net merchant dashboard. At the top left is the Authorize.Net logo. At the top right, it says "Welcome: dummy dummy". Below the logo is a navigation bar with tabs for HOME, TOOLS, REPORTS, TRANSACTION SEARCH, and ACCOUNT. The ACCOUNT tab is highlighted with a red box. Below the navigation bar is a yellow banner that reads "Your account is in TEST MODE - To update click here." Below the banner is the "Settings" page. The page has a "Settings" heading and a "Help" link. Below the heading is a paragraph: "The following sections provide access to your payment gateway integration and Merchant Interface settings. For help with configuring these settings, click the Help link in the top right corner of each settings page." Below this paragraph are three sections: "Transaction Format Settings", "Transaction Response Settings", and "Security Settings". Each section contains a list of links. The "Transaction Format Settings" section includes links for "Virtual Terminal", "Payment Form", "Upload Transaction File Format", and "Partial Authorization". The "Transaction Response Settings" section includes links for "Transaction Version", "Response/Receipt URLs", "Silent Post URL", "Email Receipt", "Receipt Page", "Relay Response", "Direct Response", and "FDS Customer Response". The "Security Settings" section includes links for "Fraud Settings", "Enhanced Card Code Verification", "Daily Velocity", "Enhanced Address Verification Service", "Cardholder Authentication", "General Security Settings", "Test Mode", "API Credentials & Keys", "Mobile Device Management", "File Upload Capabilities", "Manage Public Client Key", and "Authorized Applications".

7. Click Settings > API Credentials & Keys.

Authorize.Net

Welcome: dummy dummy

HOME TOOLS REPORTS TRANSACTION SEARCH ACCOUNT

**Settings**

- Merchant Profile
- Billing Information
- Statements
- Verified Merchant Seal
- User Administration
- User Profile
- Digital Payment Solutions

Your account is in TEST MODE - To update click here.

### Settings [Help](#)

The following sections provide access to your payment gateway integration and Merchant Interface settings. For help with configuring these settings, click the Help link in the top right corner of each settings page.

#### Transaction Format Settings

- Transaction Submission Settings
  - [Virtual Terminal](#)
  - [Payment Form](#)
  - [Upload Transaction File Format](#)
  - [Partial Authorization](#)
- Transaction Response Settings
  - [Transaction Version](#)
  - [Response/Receipt URLs](#)
  - [Receipt Page](#)
  - [Relay Response](#)
  - [Silent Post URL](#)
  - [Direct Response](#)
  - [Email Receipt](#)
  - [FDS Customer Response](#)

#### Security Settings

- Fraud Settings
  - [Enhanced Card Code Verification](#)
  - [Daily Velocity](#)
  - [Enhanced Address Verification Service](#)
  - [Cardholder Authentication](#)
- General Security Settings
  - [Test Mode](#)
  - [API Credentials & Keys](#)
  - [Mobile Device Management](#)
  - [File Upload Capabilities](#)
  - [Manage Public Client Key](#)
  - [Authorized Applications](#)

#### Business Settings

- General Information Settings
  - [Transaction Cut-Off Time](#)
  - [QuickBooks Download Report Settings](#)
  - [Time Zone](#)
- Notification Settings
  - [Webhooks](#)

8. Select New Transaction Key, and click on submit.

Note: When obtaining a new Transaction Key, you may choose to disable the old Transaction Key by clicking the box titled, Disable Old Transaction Key Immediately. You may want to do this if you suspect your previous Transaction Key is being used fraudulently.

Your account is in TEST MODE - To update click here.

**Settings**

- Merchant Profile
- Billing Information
- Statements
- Verified Merchant Seal
- User Administration
- User Profile
- Digital Payment Solutions

## API Credentials & Keys [Help](#)

Your API Login ID and Transaction Key are unique pieces of information specifically associated with your payment gateway account. However, the API login ID and Transaction Key are NOT used for logging into the Merchant interface. These two values are only required when setting up an Internet connection between your e-commerce Web site and the payment gateway. They are used by the payment gateway to authenticate that you are authorized to submit Web site transactions.

A Signature Key is applicable if your solution uses our hosted payment form, or uses the Direct Post Method (DPM) to submit transactions. It is also used for authenticating transaction responses from our APIs, including but not limited to Relay Response and Silent Post.

**IMPORTANT:** The API Login ID, Transaction Key and Signature Key should not be shared with anyone. Be sure to store these values securely and change the Transaction Key regularly to further strengthen the security of your account.

For more information about the API Login ID, Transaction Key and Signature Key, please refer to the [Reference & User Guides](#) or contact your Web developer.

API Login ID:	4b29459xcMUW
API Login ID Last Obtained:	03/12/2021 02:51:05
Transaction Key Last Obtained:	03/12/2021 02:51:00

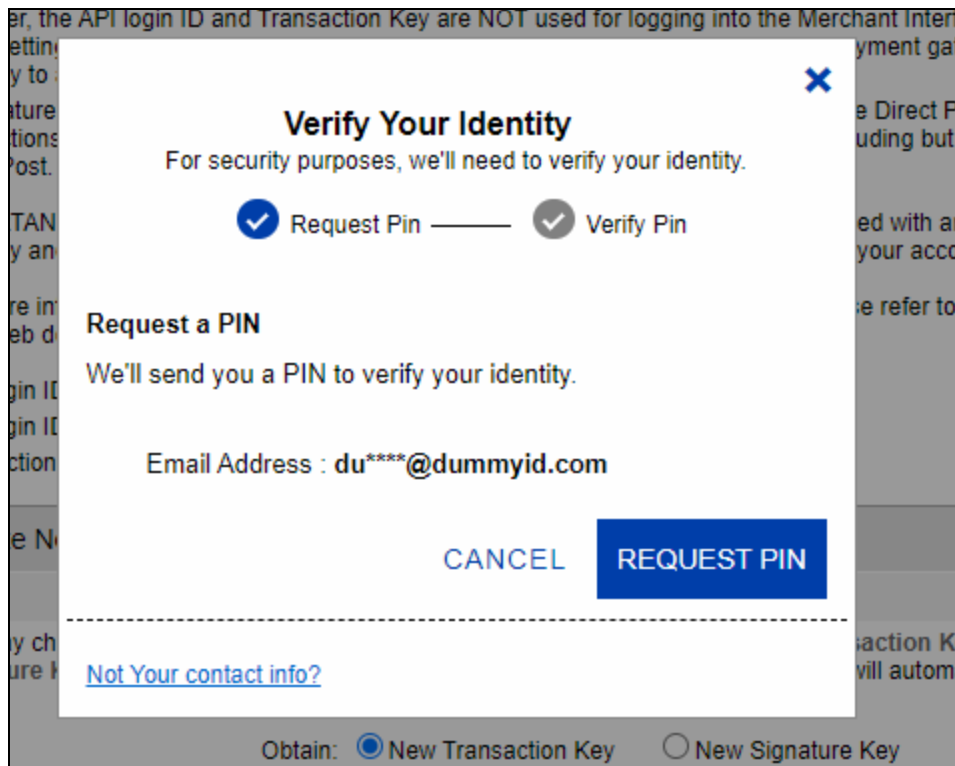
Create New Key(s) \* Required Fields

You may choose to disable the old one immediately by checking the Disable Old Transaction Key Immediately or Disable Old Signature Key Immediately option. If you do not immediately disable the old value, it will automatically expire in 24 hours.

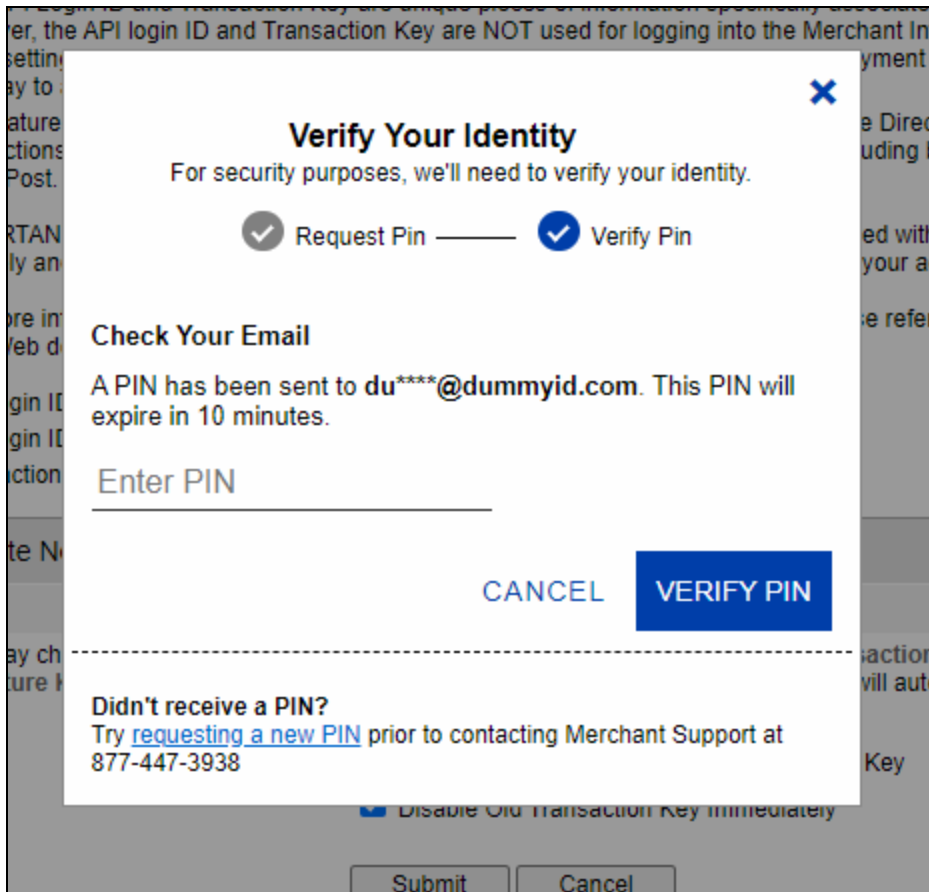
Obtain:  New Transaction Key  New Signature Key

9. A pop-up window will open. Click on the Request Pin button.





10. Next pop-up will open asking for a pin. You will get a pin on the email id used for registration. Copy and paste it. Click on verify.



er, the API login ID and Transaction Key are NOT used for logging into the Merchant Int  
setting  
ay to  
ature  
ctions  
Post.

RTAN  
ly an

ore in  
Web d

gin ID  
gin ID  
action

te N

ay ch  
ture

action  
will auto  
Key

Disable Old Transaction Key Immediately

Submit Cancel

**Verify Your Identity**

For security purposes, we'll need to verify your identity.

Request Pin  Verify Pin

**Check Your Email**

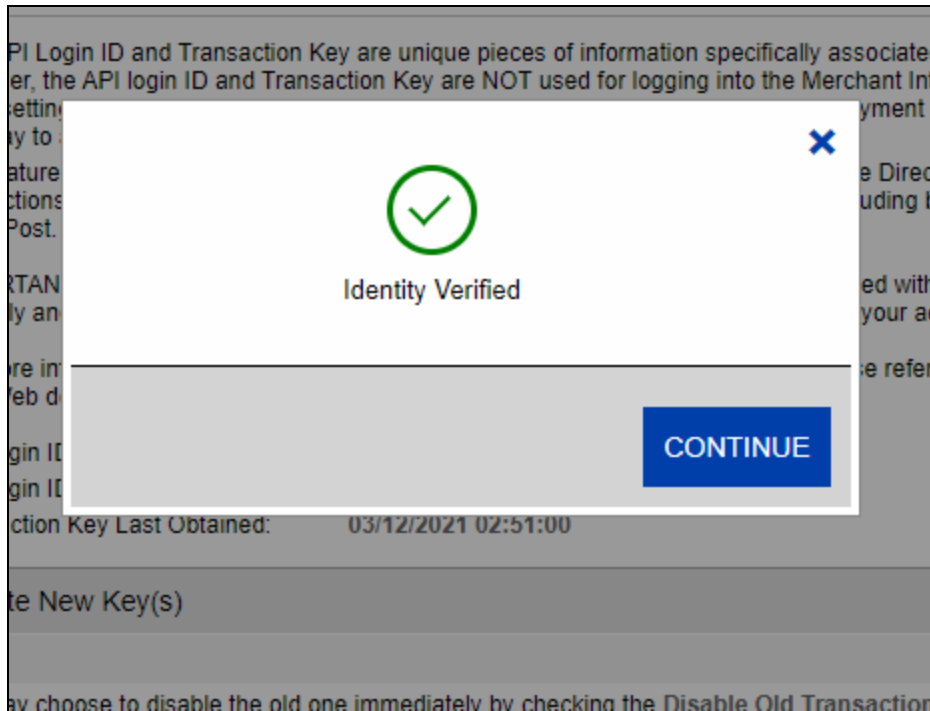
A PIN has been sent to du\*\*\*\*@dummyid.com. This PIN will expire in 10 minutes.

Enter PIN

CANCEL VERIFY PIN

**Didn't receive a PIN?**  
Try [requesting a new PIN](#) prior to contacting Merchant Support at 877-447-3938

11. Pin verified, click on continue.



12. Copy transaction key and click on continue. Now click on the same Settings->API Credentials & Keys. API Login ID is there. Save these credentials in the corresponding section of the website admin panel.

**Authorize.Net**

HOME TOOLS

**Settings**

- Merchant Profile
- Billing Information
- Statements
- Verified Merchant Seal
- User Administration
- User Profile
- Digital Payment Solutions

## API Credentials & Keys

Your API Login ID and Transaction Key are used to authenticate your system to the Authorize.Net API. However, the API login ID and Transaction Key are not used when setting up an Internet connection gateway to authenticate that you are a merchant.

A Signature Key is applicable if your system is used for processing transactions. It is also used for authenticating Silent Post.

**IMPORTANT:** The API Login ID, Transaction Key, and Signature Key should be stored securely and change the Transaction Key regularly.

For more information about the API Login ID and Transaction Key, contact your Web developer.

API Login ID:  
 API Login ID Last Obtained:  
 Transaction Key Last Obtained:

[Create New Key\(s\)](#)

You may choose to disable the old on the [Signature Key Immediately](#) option. [Obtain](#)

13. Important: Right now in system, MD5 hash is optional and not in use. So below points (Point 14) are just for knowledge's sake. (As when signature key concept will be implemented in system, Point 14 will necessary to perform)

Note: MD5 Hash concept is ended now, and signature key concept added as a replacement of it. As stated in the support forum link: (<https://support.authorize.net/s/article/MD5-Hash-End-of-Life-Signature-Key-Replacement>). (Right now in system md5 or signature key concept is not in use)

Authorize.Net is phasing out the MD5 based hash use for transaction response verification in favor of the SHA-512 based hash utilizing a Signature Key.

The end of life for MD5 Hash will be done in two phases:

Phase 1 - As of February 11, 2019 Authorize.net have removed the ability to configure or update MD5 Hash setting in the Merchant Interface. Merchants who had this setting configured have already been emailed/contacted.

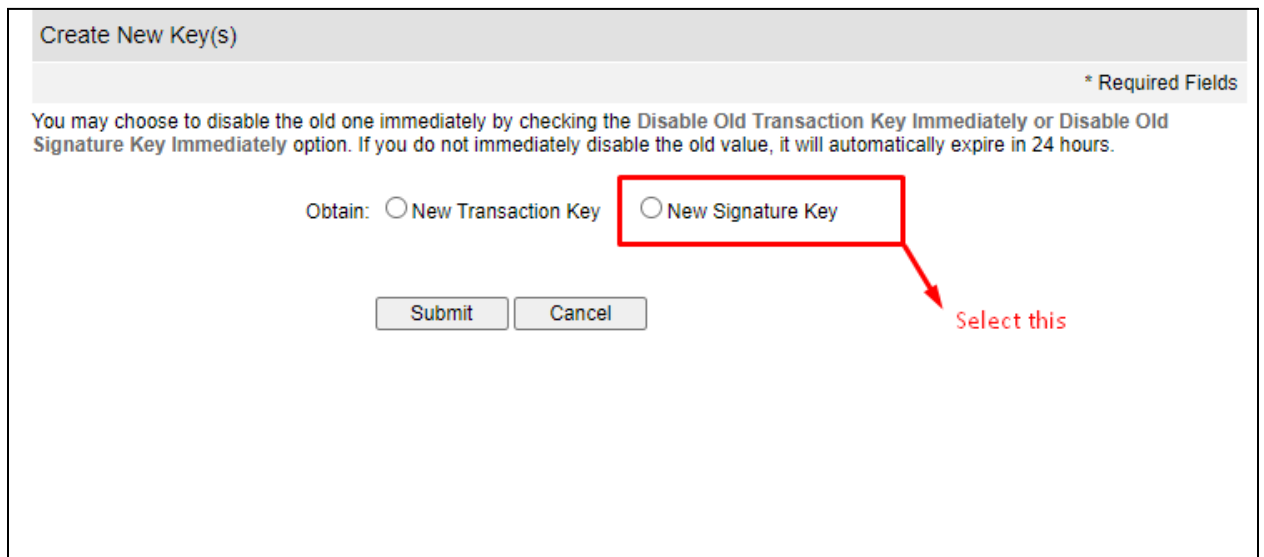
Phase 2 - Stop sending the MD5 Hash data element in the API response. To continue verifying via hash, this will require applications to support the SHA-512 hash via signature key.

- Sandbox has been updated as of March 7, 2019 to stop populating the MD5 Hash value, but the field will still be present but empty.
- Production has been updated as of June 27, 2019 (10:30am PT) to stop populating the MD5 Hash value, but the field will still be present but empty.

When you receive a transaction response from [Authorize.Net](#), it includes a SHA2 hash element, the name and position depend on the API integration method used.

The SHA2 field contains HMAC-SHA512 hash that [Authorize.Net](#) generated for the transaction and can be used to validate the response came from [Authorize.Net](#) but is not required to do so.

14. To obtain 'Signature key' follow the same process from Point 6 to 12 but select 'new signature key' instead of 'new transaction key'



Create New Key(s)

\* Required Fields

You may choose to disable the old one immediately by checking the Disable Old Transaction Key Immediately or Disable Old Signature Key Immediately option. If you do not immediately disable the old value, it will automatically expire in 24 hours.

Obtain:  New Transaction Key  New Signature Key

Submit Cancel

Select this

This signature key needs to be added instead of Md5 hash into the system once implemented in the system.